Forum aux questions sur QoS (Qualité de service)

Table des matières

[Introduction](#)
[Généralités](#)
[Classification et marquage](#)
[Gestion de la congestion et de la mise en file d'attente](#)
[Weighted Random Early Detection (WRED) en prévention de congestion](#)
[Réglementation et formatage](#)
[Qualité de service (QoS) des relais de trame](#)
[Qualité de service (QoS) sur mode de transfert asynchrone (ATM)](#)
[Voix et qualité de service (QoS)](#)
[Informations connexes](#)

Introduction

Ce document répond aux questions les plus fréquentes (Forum aux questions) relatives à la qualité de service (QoS).

Généralités

Q. Qu'est-ce que la qualité de service (QoS) ?

R. La qualité de service (QoS) désigne la capacité d'un réseau à fournir un meilleur service au trafic réseau sélectionné sur diverses technologies sous-jacentes, notamment les réseaux Frame Relay, ATM (Asynchronous Transfer Mode), Ethernet et 802.1, SONET et les réseaux routés IP.

La QoS consiste en un ensemble de technologies qui permettent à des applications de demander et recevoir des niveaux de service prévisibles en termes de capacité de débit de données (bande passante), variations de latence (jitter) et de délais. En particulier, les fonctions QoS offrent un meilleur service réseau, plus prévisible, à l'aide des méthodes suivantes :

- Prise en charge de bande passante dédiée.
- Amélioration des caractéristiques de perte.
- Prévention et gestion de la congestion du réseau.
- Formatage du trafic réseau.
- Définition des priorités de trafic sur le réseau.

L'Internet Engineering Task Force (IETF) définit les deux architectures suivantes pour la QoS :

- Services intégrés (IntServ)
- Services différenciés (DiffServ)

IntServ utilise le Resource Reservation Protocol (RSVP) pour signaler explicitement les besoins en QoS du trafic d'une application sur les périphériques du chemin d'accès de bout en bout via le réseau. Si chaque périphérique réseau du chemin d'accès peut réserver la bande passante nécessaire, l'application d'origine peut commencer à transmettre. La RFC 2205 définit le RSVP et la RFC 1633 définit les services IntServ.

DiffServ met l'accent sur la QoS agrégée et dimensionnée. Au lieu de signaler les besoins d'une application en termes de QoS, DiffServ utilise un point de code de services différenciés (DSCP) dans l'en-tête IP pour indiquer les niveaux de QoS requis. La conformité DiffServ sur les routeurs Cisco a été introduite par la version 12.1(5)T du logiciel Cisco IOS®. Pour plus d'informations, référez-vous aux documents suivants :

- Service intégré dans Cisco IOS 12.1
- Mise en œuvre de DiffServ pour la qualité de service de bout en bout
- Implémentation de stratégies de qualité de service avec le point de code de services différenciés (DSCP)

Q. Que sont la congestion, le délai et la gigue ?

R. Une interface est encombrée lorsqu'elle reçoit plus de trafic qu'elle ne peut en gérer. Les points de congestion du réseau sont de solides candidats pour les mécanismes de qualité de service (QoS). Voici un exemple de points de congestion classiques :

La congestion d'un réseau entraîne des délais. Un réseau et ses périphériques présentent plusieurs types de délais, comme expliqué dans Présentation des délais dans les réseaux de paquets voix. Une variation de délai est appelée gigue, comme expliqué dans Présentation des gigues dans les réseaux de paquets voix (plates-formes Cisco IOS). Les phénomènes de délai et de gigue doivent être contrôlés et minimisés de façon à pouvoir prendre en charge un trafic interactif et en temps réel.

Q. Qu'est-ce que le MQC ?

R. MQC est l'acronyme de Qualité de service (QoS) modulaire Command Line Interface (CLI). Elle est destinée à simplifier la configuration de la QoS sur les routeurs et les commutateurs Cisco en définissant une syntaxe de commandes commune et un ensemble de comportements de QoS résultant sur toutes les plates-formes. Ce modèle remplace la version précédente qui consistait à définir des syntaxes uniques pour chaque fonction QoS et pour chaque plate-forme.

La MQC comprend les trois étapes suivantes :

1. Définir une classe de trafic en émettant la commande class-map.

2. Créer une stratégie de trafic en associant la classe de trafic à une ou plusieurs fonctions QoS à l'aide de la commande policy-map.

3. Lier la stratégie de trafic à l'interface, à la sous-interface ou au circuit virtuel à l'aide de la commande service-policy.

Remarque : vous implémentez les fonctions de conditionnement du trafic de DiffServ, telles que le marquage et la mise en forme, à l'aide de la syntaxe MQC.

Pour plus d'informations, consultez Interface de ligne de commande de qualité de service modulaire.

Q. Que signifie la `politique de service prise en charge uniquement sur les interfaces VIP avec le` message `DCEF activé` ?

R. Sur les VIP (Versatile Interface Processors) d'un Cisco 7500, seules les fonctionnalités de qualité de service (QoS) distribuées sont prises en charge dans Cisco IOS 12.1(5)T, 12.1(5)E et 12.0(14)S. L'activation de la technologie Cisco Express Forwarding (dCEF) distribuée active automatiquement la QoS distribuée.

Les interfaces autres que VIP, appelées processeurs d'interface hérités (IPS), prennent en charge les fonctions QoS centrales telles qu'activées sur les processeurs de commutation routage (RSP). Pour plus d'informations, référez-vous aux documents suivants :

- Mise en file d'attente pondérée basée sur les classes (CBWFQ) distribuée et Weighted Random Early Detection (WRED) distribuée
- Low Latency Queueing distribué
- Formatage du trafic distribué
- FRF.11 et FRF.12 Versatile Interface Processor distribués pour Cisco IOS Version 12.1 T

Q. Combien de classes une politique de qualité de service (QoS) prend-elle en charge ?

R. Dans les versions de Cisco IOS antérieures à la version 12.2, vous ne pouviez définir qu'un maximum de 256 classes, et vous pouviez définir jusqu'à 256 classes dans chaque politique si les mêmes classes sont réutilisées pour des politiques différentes. Si vous avez deux stratégies, le nombre total de classes des deux stratégies ne doit pas dépasser 256. Si une stratégie inclut la mise en file d'attente pondérée basée sur les classes (CBWFQ) (ce qui signifie qu'elle contient une instruction bandwidth [ou priority] dans l'une des classes), le nombre total de classes prises en charge est 64.

Dans Cisco IOS Versions 12.2(12), 12.2(12)T et 12.2(12)S, cette limitation de 256 mappages de classes globales a été modifiée. Il est maintenant possible de configurer jusqu'à 1 024 mappages de classes globales et d'utiliser 256 mappages de classes à l'intérieur du même mappage de stratégies.

Q. Comment les mises à jour de routage et les keepalives PPP (Point-to-Point Protocol) / HDLC (High-Level Data Link Control) sont-elles traitées lorsqu'une stratégie de service est appliquée ?

R. Les routeurs Cisco IOS utilisent les deux mécanismes suivants pour hiérarchiser les paquets de contrôle :

- Priorité IP
- pak_priority

Les deux mécanismes sont conçus pour s'assurer que des paquets de contrôle de clé ne sont pas supprimés ou qu'ils sont supprimés en dernier par le routeur et le système de mise en file d'attente lorsqu'une interface de sortie est congestionnée. Pour plus d'informations, consultez Comprendre comment les mises à jour de routage et les paquets de contrôle sont mis en file d'attente sur une interface avec une stratégie de service QoS.

Q. La qualité de service (QoS) est-elle prise en charge sur les interfaces configurées avec le routage et le pontage intégrés (IRB) ?

R. Non. Vous ne pouvez pas configurer les fonctions QoS lorsque l'interface est configurée pour IRB.

Classification et marquage

Q. Qu'est-ce que la préclassification de la qualité de service (QoS) ?

R. La préclassification QoS vous permet de faire correspondre et de classer le contenu d'en-tête IP d'origine des paquets soumis à l'encapsulation et/ou au cryptage de tunnel. Cette fonction ne décrit pas le processus de copie de la valeur initiale de l'octet de type de service (ToS) de l'en-tête du paquet d'origine dans l'en-tête du tunnel. Pour plus d'informations, référez-vous aux documents suivants :

- Configuration de la QoS pour les réseaux privés virtuels
- Qualité de service pour les réseaux privés virtuels, module fonctionnel 12.2(2)T

Q. Quels champs d'en-tête de paquet peuvent être notés ? Quelles sont les valeurs disponibles ?

R. La fonction de marquage par classe vous permet de définir ou de marquer l'en-tête de couche 2, de couche 3 ou MPLS (Multiprotocol Label Switching) de vos paquets. Pour plus d'informations, référez-vous aux documents suivants :

- Configuration du marquage de paquets basé sur les classes
- Quand un routeur définit-il le bit CLP dans une cellule ATM ?

- Configuration du marquage de paquet sur PVC de relais de trame

Q. Puis-je hiérarchiser le trafic en fonction de l'URL ?

R. Oui. La Network Based Application Recognition (NBAR) permet de classer les paquets en fonction de la correspondance des champs de la couche applicative. Avant l'introduction de NBAR, la classification la plus précise était basée sur les numéros de port TCP et UDP de la couche 4. Pour plus d'informations, référez-vous aux documents suivants :

- Questions et réponses relatives à la Network-Based Application Recognition (NBAR)
- Mise en réseau d'applications NBAR
- Utilisation des listes de contrôle d'accès et de NBAR pour bloquer le ver Code Red
- Comment protéger votre réseau contre le virus Nimda

Q. Quelles plates-formes et versions du logiciel Cisco IOS prennent en charge NBAR (Network Based Application Recognition) ?

R. La prise en charge de NBAR est introduite dans les versions suivantes du logiciel Cisco IOS :

Plateforme	Version logicielle Cisco IOS minimale
7200	12.1(5)T
7100	12.1(5)T
3660	12.1(5)T
3640	12.1(5)T
3620	12.1(5)T
2600	12.1(5)T
1700	12.2(2)T

Remarque : vous devez activer Cisco Express Forwarding (CEF) pour utiliser NBAR.

La NBAR distribuée (DNBAR) est disponible sur les plates-formes suivantes :

Plateforme	Version logicielle Cisco IOS minimale
7500	12.2(4)T, 12.1(6)E
FlexWAN	12.1(6)E

Remarque : NBAR n'est pas pris en charge sur les interfaces VLAN MSFC (Multilayer Switch Feature Card) du Catalyst 6000, sur la gamme Cisco 12000 ou sur le module RSM (Route Switch Module) du Catalyst 5000. Si vous ne trouvez pas une plate-forme particulière dans la liste ci-dessus, contactez le représentant du support technique Cisco.

Gestion de la congestion et de la mise en file d'attente

Q. Quel est l'objectif de la mise en file d'attente ?

R. La mise en file d'attente est conçue pour gérer l'encombrement temporaire sur l'interface d'un périphérique réseau en stockant les paquets excédentaires dans des tampons jusqu'à ce que la bande passante devienne disponible. Les routeurs Cisco IOS prennent en charge plusieurs méthodes de mise en file d'attente de façon à répondre aux besoins variables en termes de bande passante, de gigue et de délai des différentes applications.

Le mécanisme par défaut sur la plupart des interfaces est la mise en file d'attente First In First Out (FIFO). Certains types de trafics sont plus exigeants en termes de délai/gigue. Ainsi, l'un des autres mécanismes de mise en file d'attente suivants doit être configuré ou est activé par défaut :

- Mise en file d'attente pondérée (WFQ)
- Mise en file d'attente pondérée basée sur les classes (CBWFQ)
- Low Latency Queueing (LLQ), qui est en fait une CBWFQ avec une file d'attente par priorité (PQ) (appelée PQCBWFQ)
- Mise en file d'attente par priorité (PQ)
- Mise en file d'attente personnalisée (CQ)

La mise en file d'attente se produit généralement uniquement sur les interfaces de sortie. Un routeur place en file d'attente les paquets qui sortent d'une interface. Vous pouvez réglementer le trafic entrant, mais vous ne pouvez généralement pas le mettre en file d'attente (à l'exception de la mise en mémoire tampon côté réception sur un routeur de la gamme Cisco 7500 utilisant la technologie Cisco Express Forwarding (CEF) distribuée pour transférer des paquets de l'interface d'entrée vers l'interface de sortie ; pour plus d'informations, consultez Présentation du CPU VIP s'exécutant à 99 % et de la mise en mémoire tampon Rx-Side. Sur les plates-formes distribuées de pointe, telles que les gammes Cisco 7500 et 12000, l'interface d'entrée peut utiliser ses propres mémoires tampon de paquets pour stocker le trafic excédentaire commuté vers une interface de sortie congestionnée suite à la décision de commutation de l'interface d'entrée. Dans de rares conditions, généralement quand l'interface d'entrée alimente une interface de sortie plus lente, l'interface d'entrée peut être confrontée à un nombre croissant d'erreurs ignorées lorsqu'elle manque de mémoire de paquets. Une congestion excessive peut engendrer la suppression de la file d'attente de sortie. Les suppressions de files d'attente d'entrée ont généralement une cause d'origine différente. Pour plus d'informations sur le dépannage des suppressions, consultez le document suivant :

- Dépannage des suppressions dans la file d'attente d'entrée et de sortie

Pour plus d'informations, référez-vous aux documents suivants :

- Dépannage des erreurs « Ignored » sur un adaptateur de port ATM

- Dépannage des erreurs ignorées et des suppressions dues au manque de mémoire sur les routeurs Internet de la gamme Cisco 12000

Q. Comment fonctionnent la mise en file d'attente pondérée (WFQ) et la mise en file d'attente pondérée basée sur les classes (CBWFQ) ?

R. La mise en file d’attente équitable vise à allouer une part équitable de la bande passante d’une interface entre les conversations actives ou les flux IP. Elle classe les paquets en sous-files d'attente, identifiées par un numéro d'identification de conversation, utilisant un algorithme de hachage basé sur plusieurs champs de l'en-tête IP et la longueur du paquet. La pondération est calculée de la façon suivante :

- W=K/(priorité +1)

K= 4 096 avec Cisco IOS 12.0(4)T et les versions antérieures, et 32 384 avec 12.0(5)T et les versions ultérieures.

Plus la pondération est faible, plus la priorité et le partage de la bande passante sont élevés. En plus de la pondération, la longueur du paquet est prise en considération.

CBWFQ permet de définir une classe de trafic et de lui attribuer une garantie de bande passante minimale. L'algorithme derrière ce mécanisme est WFQ, qui explique le nom. Pour configurer CBWFQ, vous définissez des classes spécifiques dans des instructions de classes de mappage. Vous affectez ensuite une stratégie à chaque classe dans un mappage de stratégie. Ce mappage de stratégie sera alors attaché en sortie à une interface. Pour plus d'informations, référez-vous aux documents suivants :

- Présentation de la mise en file d'attente pondérée basée sur les classes sur les interfaces ATM
- Présentation de la mise en file d'attente pondérée (WFQ) sur des interfaces ATM

Q. Si une classe CBWFQ (Class Based Weighted Fair Queueing) n'utilise pas sa bande passante, d'autres classes peuvent-elles utiliser la bande passante ?

R. Oui. Bien que les garanties de bande passante fournies par les commandes bandwidth et priority aient été décrites avec des mots tels que « réservé » et « bande passante à mettre de côté », aucune de ces commandes ne met en œuvre une vraie réservation. En d'autres termes, si une classe de trafic n'utilise pas sa bande passante configurée, n'importe quelle bande passante inutilisée est partagée parmi les autres classes.

Le système de mise en file d'attente impose une importante exception à la règle avec une classe prioritaire. Comme noté ci-dessus, la charge offerte d'une classe prioritaire est dosée par un régulateur de trafic. Pendant les états d'encombrement, une classe prioritaire ne peut utiliser aucune bande passante excessive. Pour plus d'informations, reportez-vous à Comparaison des commandes bandwidth et priority d'une stratégie de service QoS.

Q. CBWFQ (Class Based Weighted Fair Queueing) est-il pris en charge sur les sous-interfaces ?

R. Les interfaces logiques Cisco IOS ne prennent pas en charge de manière inhérente un état d'encombrement et ne prennent pas en charge l'application directe d'une stratégie de service qui applique une méthode de mise en file d'attente. Au lieu de cela, vous devez d'abord appliquer le formatage à la sous-interface à l'aide du Generic Traffic Shaping (GTS) ou du formatage basé sur les classes. Pour plus d'informations, consultez Application des fonctions QoS aux sous-interfaces Ethernet.

Q. Quelle est la différence entre les instructions `priority` et `bandwidth` dans un policy-map ?

R. Les commandes priority et bandwidth diffèrent à la fois par leur fonctionnalité et par les applications qu'elles prennent généralement en charge. Le tableau suivant récapitule ces différences :

Fonction	commande bandwidth	commande priority
Garantie de bande passante minimale	Oui	Oui
Garantie de bande passante maximale	Non	Oui
Contrôle intégré	Non	Oui
Fournit une faible latence	Non	Oui

Pour plus d'informations, reportez-vous à Comparaison des commandes bandwidth et priority d'une stratégie de service QoS.

Q. Comment la limite de file d'attente est-elle calculée sur le FlexWAN et les processeurs VIP (Versatile Interface Processors) ?

R. En supposant une mémoire SRAM suffisante sur le VIP ou FlexWAN, la limite de file d'attente est calculée sur la base d'un délai maximal de 500 ms avec une taille moyenne de paquet de 250 octets. Voici l'exemple d'une classe avec un Mbits/s de bande passante :

Limite de file d'attente = 1000000/(250 x 8 x 2) = 250

À mesure que la quantité de mémoire de paquets disponible diminue, des limites de file d'attente plus petites sont attribuées, avec un nombre plus grand de circuits virtuels (VC).

Dans l'exemple suivant, un PA-A3 est installé dans une carte FlexWAN de la gamme Cisco 7600 et prend en charge plusieurs sous-interfaces avec des circuits virtuels permanents de 2 Mo (PVC).

La stratégie de service est appliquée à chaque circuit virtuel.

<#root>

```
class-map match-any XETRA-CLASS
  match access-group 104
class-map match-any SNA-CLASS
  match access-group 101
  match access-group 102
  match access-group 103
policy-map
```

POLICY-2048Kbps

```
  class XETRA-CLASS
    bandwidth 320
  class SNA-CLASS
    bandwidth 512

interface ATM6/0/0
 no ip address
 no atm sonet ilmi-keepalive
 no ATM ilmi-keepalive
!
interface ATM6/0/0.11 point-to-point
 mtu 1578
 bandwidth 2048
 ip address 22.161.104.101 255.255.255.252
 pvc ABCD
  class-vc 2048Kbps-PVC
  service-policy out
```

POLICY-2048Kbps

L'interface de mode de transfert asynchrone (ATM) obtient une limite de file d'attente pour l'intégralité de l'interface. La limite est une fonction calculant la quantité totale de mémoire tampon disponible, le nombre d'interfaces physiques sur le FlexWAN et le délai de mise en file d'attente maximal autorisé sur l'interface. Chaque PVC obtient une partie de la limite d'interface en fonction du Sustained Cell Rate (SCR) ou du Minimum Cell Rate (MCR) du PVC, et chaque classe obtient une partie de la limite de PVC en fonction de son allocation de bande passante.

L'exemple de sortie suivant de la commande show policy-map interface est dérivé d'un FlexWAN avec 3687 mémoires tampon globales. Émettez la commande show buffer pour obtenir cette valeur. 50 paquets sont alloués à chaque PVC de 2 Mbits/s en fonction de la bande passante du PVC de 2 Mbits/s (2047/149760 x 3687 = 50). Une partie des 50 paquets est ensuite allouée à chaque classe, comme le montre l'exemple suivant :

<#root>

```
service-policy output: POLICY-2048Kbps
    class-map: XETRA-CLASS (match-any)
      687569 packets, 835743045 bytes
      5 minute offered rate 48000 bps, drop rate 6000 BPS
```

```
      match: access-group 104
        687569 packets, 835743045 bytes
        5 minute rate 48000 BPS
      queue size 0,
```

queue limit 7

```
      packets output 687668, packet drops 22
      tail/random drops 22, no buffer drops 0, other drops 0
      bandwidth: kbps 320, weight 15

    class-map: SNA-CLASS (match-any)
      2719163 packets, 469699994 bytes
      5 minute offered rate 14000 BPS, drop rate 0 BPS
      match: access-group 101
        1572388 packets, 229528571 bytes
        5 minute rate 14000 BPS
      match: access-group 102
        1146056 packets, 239926212 bytes
        5 minute rate 0 BPS
      match: access-group 103
        718 packets, 245211 bytes
        5 minute rate 0 BPS
      queue size 0,
```

queue limit 12

```
      packets output 2719227, packet drops 0
      tail/random drops 0, no buffer drops 0, other drops 0
      bandwidth: kbps 512, weight 25
      queue-limit 100

    class-map: class-default (match-any)
      6526152 packets, 1302263701 bytes
      5 minute offered rate 44000 BPS, drop rate 0 BPS
      match: any
        6526152 packets, 1302263701 bytes
        5 minute rate 44000 BPS
      queue size 0,
```

queue limit 29

```
      packets output 6526840, packet drops 259
      tail/random drops 259, no buffer drops 0, other drops 0
```

Si vos flux de trafic utilisent de grandes tailles de paquet, le résultat de la commande show policy-map interface peut signaler une valeur à incrémentation pour les champs `no buffer drops dans la mesure où vous pouvez manquer de mémoires tampon avant d'atteindre la limite de la file d'attente`. Dans ce cas, essayez de diminuer manuellement les classes queue-limit et non-priority. Pour plus d'informations, consultez Présentation de la transmission de la limite de file d'attente avec CoS IP à ATM.

Q. Comment vérifiez-vous la valeur queue-limit ?

R. Sur les plates-formes non distribuées, la limite de file d'attente est de 64 paquets par défaut.

L'exemple de résultat suivant a été capturé sur un routeur de la gamme Cisco 3600 :

```
<#root>

november#

show policy-map interface s0


   Serial0

   Service-policy output: policy1

     Class-map: class1 (match-all)
       0 packets, 0 bytes
       5 minute offered rate 0 BPS, drop rate 0 BPS
       Match: ip precedence 5
       Weighted Fair Queueing
         Output Queue: Conversation 265
         Bandwidth 30 (kbps) Max Threshold 64 (packets)

!--- Max Threshold is the queue-limit.

          (pkts matched/bytes matched) 0/0
          (depth/total drops/no-buffer drops) 0/0/0

      Class-map: class2 (match-all)
        0 packets, 0 bytes
        5 minute offered rate 0 BPS, drop rate 0 BPS
        Match: ip precedence 2
        Match: ip precedence 3
        Weighted Fair Queueing
          Output Queue: Conversation 266
          Bandwidth 24 (kbps) Max Threshold 64 (packets)
          (pkts matched/bytes matched) 0/0
          (depth/total drops/no-buffer drops) 0/0/0

       Class-map: class-default (match-any)
         0 packets, 0 bytes
         5 minute offered rate 0 BPS, drop rate 0 BPS
         Match: any
```

Q. Puis-je activer la mise en file d'attente équitable dans une classe ?

R. La gamme Cisco 7500 avec qualité de service (QoS) distribuée prend en charge une mise en file d’attente équitable par classe. D'autres plates-formes, y compris la gamme Cisco 7200 et la gamme Cisco 2600/3600, prennent en charge la mise en file d'attente pondérée (WFQ) dans la classe class-default ; toutes les classes de bande passante utilisent le mécanisme First In First Out (FIFO).

Q. Quelles commandes puis-je utiliser pour surveiller la mise en file d’attente ?

R. Utilisez les commandes suivantes pour surveiller la mise en file d'attente :

- show queue {interface} {numéro d'interface} - sur des plateformes Cisco IOS autres que la gamme Cisco 7500, cette commande affiche les files d'attente ou les conversations actives. Si l'interface ou le circuit virtuel n'est pas congestionné, aucune file d'attente ne sera listée. Sur la gamme Cisco 7500, la commande show queue n'est pas prise en charge.

- show queueing interface interface-number [vc [[vpi/] vci] - cette commande affiche les statistiques de mise en file d'attente sur une interface ou un circuit virtuel. Même s'il n'y a aucune congestion, vous pourrez toujours voir quelques accès ici. Les paquets commutés par les processus sont toujours pris en compte qu'il y ait ou non congestion. Cisco Express Forwarding (CEF) et les paquets à commutation rapide ne sont pas pris en compte sauf s'il y a congestion. Les mécanismes de mise en file d'attente habituels comme la mise en file d'attente par priorité (PQ), la mise en file d'attente personnalisée (CQ) et la mise en file d'attente pondérée (WFQ) ne fournissent pas de statistiques de classification. Seules les fonctionnalités Modular QoS CLI (MQC) dans les images ultérieures à 12.0(5)T fournissent ces statistiques.

- show policy interface {interface}{numéro d'interface} - Le compteur packets compte le nombre de paquets correspondant aux critères de la classe. Ce compteur est incrémenté que l'interface soit ou ne soit pas congestionnée. Le compteur `packets matched indique le nombre de paquets correspondant aux critères de la classe quand l'interface a été congestionnée`. Pour plus d'informations sur les compteurs de paquets, consultez le document suivant :

  Présentation des compteurs de paquets dans la sortie d'interface show policy-map

- MIB de statistiques et de configuration QoS basée sur les classes Cisco - Fournit des fonctionnalités de surveillance du protocole de gestion de réseau simple (SNMP).

Q. RSVP peut être utilisé conjointement avec la mise en file d'attente pondérée basée sur les classes (CBWFQ). Lorsque les protocoles Resource Reservation Protocol (RSVP) et CBWFQ sont tous deux configurés pour une interface, RSVP et CBWFQ agissent-ils de façon indépendante, en ayant le même comportement que celui qu'ils auraient si chacun d'eux s'exécutait seul ? RSVP semble se comporter comme si CBWFQ n'était pas configuré en termes de disponibilité, d'estimation et d'allocation de bande passante.

R. Lors de l'utilisation de RSVP et CB-WFQ dans le logiciel Cisco IOS Version 12.1(5)T et ultérieure, le routeur peut fonctionner de telle sorte que les flux RSVP et les classes CBWFQ partagent la bande passante disponible sur une interface ou un circuit virtuel permanent, sans surabonnement.

La version logicielle d'IOS 12.2(1)T et versions ultérieures permet au RSVP d'effectuer un contrôle d'admission en utilisant son propre pool « ip rsvp bandwidth », tandis que la CBWFQ gère la classification, la réglementation et la planification des paquets RSVP. Cela suppose que les paquets soient prémarqués par l'expéditeur et que les paquets non RSVP soient marqués différemment.

Weighted Random Early Detection (WRED) en prévention de congestion

Q. Puis-je activer simultanément la détection WRED (Weighted Random Early Detection) et LLQ (Low Latency Queueing) ou CBWFQ (Class Based Weighted Fair Queueing) ?

R. Oui. La mise en file d'attente définit l'ordre dans lequel les paquets sortent de la file d'attente. En d'autres termes, elle définit un mécanisme de planification des paquets. Elle peut également être utilisée pour fournir une allocation de bande passante équitable et des garanties de bande passante minimales. En revanche, la RFC 2475 définit la suppression comme le « processus de suppression des paquets en fonction de règles spécifiées ». Le « tail-drop » constitue le mécanisme de suppression par défaut, dans lequel l'interface supprime les paquets lorsque la file d'attente est pleine. La détection précoce aléatoire (RED) et la WRED de Cisco constituent d'autres mécanismes de suppression, lesquels suppriment des paquets de façon aléatoire avant que la file d'attente ne soit pleine et cherchent à conserver une profondeur moyenne de file d'attente cohérente. La WRED utilise la valeur de priorité IP des paquets pour prendre une décision de suppression différenciée. Pour plus d'informations, consultez Weighted Random Early Detection (WRED).

Q. Comment puis-je surveiller la détection WRED (Weighted Random Early Detection) et voir qu'elle prend réellement effet ?

R. WRED surveille la profondeur moyenne de la file d’attente et commence à supprimer des paquets lorsque la valeur calculée dépasse la valeur de seuil minimale. Émettez la commande show policy-map interface et contrôlez la valeur de la profondeur moyenne de la file d'attente, come le montre l'exemple suivant :

<#root>

```
Router#
show policy interface s2/1


  Serial2/1
  output : p1
   Class c1
    Weighted Fair Queueing
        Output Queue: Conversation 265
          Bandwidth 20 (%)
          (pkts matched/bytes matched) 168174/41370804
          (pkts discards/bytes discards/tail drops) 20438/5027748/0
          mean queue depth: 39

     Dscp      Random drop       Tail drop        Minimum   Maximum     Mark
     (Prec)     pkts/bytes        pkts/bytes      threshold threshold probability
       0(0)     2362/581052        1996/491016        20        40       1/10
       1           0/0                0/0             22        40       1/10
```

```
2          0/0                0/0              24         40        1/10
[output omitted]
```

Réglementation et formatage

Q. Quelle est la différence entre le maintien de l'ordre et le façonnage ?

R. Le diagramme suivant illustre la différence clé. Le formatage de trafic retient les paquets excédentaires dans une file d'attente, puis planifie l'excédent pour une transmission ultérieure sur des incréments de temps. Le résultat du formatage de trafic est un débit en sortie en douceur de paquets. En revanche, la réglementation du trafic propage des salves. Quand le débit de trafic atteint le débit maximal configuré, le trafic excessif est extrait (ou marqué une nouvelle fois). Le résultat est un débit en sortie qui apparaît en dents de scie avec des hauts et des bas.

Pour plus d'informations, consultez Vue d'ensemble de la réglementation et du formatage.

Q. Qu’est-ce qu’un « token bucket » et comment fonctionne l’algorithme ?

R. Un compartiment à jetons n'a pas de stratégie de suppression ou de priorité. L'exemple suivant illustre la façon dont le saut à jetons fonctionne :

- Les jetons sont placés dans le saut à un certain débit.
- Chaque jeton constitue une autorisation pour que la source envoie un certain nombre de bits.
- Pour envoyer un paquet, le régulateur de trafic doit pouvoir retirer du saut un certain nombre de jetons égal dans la représentation à la taille de paquet.
- Si le nombre de jetons dans le saut est insuffisant pour envoyer un paquet, le paquet attend que le saut ait assez de jetons (dans le cas d'un modélisateur), ou le paquet est ignoré ou démarqué (dans le cas d'un régulateur).
- Le saut lui-même a une capacité spécifique. Si le saut est totalement rempli, les jetons nouvellement arrivés sont ignorés et ne sont pas disponibles pour de futurs paquets. Ainsi, à tout moment, la plus grande rafale qu'une source peut envoyer dans le réseau est approximativement proportionnelle à la taille du saut. Un saut à jetons permet les rafales, mais les lie.

Q. Avec un régulateur de trafic tel que la réglementation basée sur les classes, que signifient Committed Burst (BC) et Excess Burst (Be) et comment dois-je sélectionner ces valeurs ?

R. Un régulateur de trafic ne met pas en mémoire tampon les paquets excédentaires et ne les transmet pas ultérieurement, comme c’est le cas pour un modélisateur. Au lieu de cela, le régulateur exécute une simple stratégie d'envoi ou de non-envoi sans mise en mémoire tampon.

Durant les périodes de congestion, puisque vous ne pouvez pas placer les paquets en mémoire tampon, la meilleure solution consiste à supprimer des paquets de façon moins agressive en configurant correctement le mode rafale étendue. Par conséquent, il est important de comprendre que le régulateur utilise les valeurs de rafale normale et de rafale étendue pour être sûr que le débit minimal garanti (CIR) soit atteint.

Les paramètres de rafale sont légèrement modelés sur la règle générique de mise en mémoire tampon destinée aux routeurs. La règle recommande de configurer la mise en mémoire tampon par rapport à la vitesse de transmission des allers-retours de façon à pouvoir accueillir les fenêtres du protocole de contrôle de transmissions (TCP) de toutes les connexions en période de congestion.

Le tableau suivant décrit l'usage et la formule recommandée pour les valeurs de rafale normales et étendues :

Paramètre de rafale	Objectif	Formule recommandée
rafale normale	• Implémente un saut à jetons standard. • Fixe la taille maximale du saut à jetons (bien que des jetons puissent être empruntés si Be est supérieur à BC). • Détermine la taille du saut à jetons dans la mesure où les nouveaux jetons sont supprimés et ne sont pas disponibles pour les futurs paquets si le saut atteint sa pleine capacité.	<#root> **CIR [BPS] * (1 byte)/(8 bits) * 1.5 seconds** Remarque : 1,5 seconde est le temps de parcours aller-retour typique.
rafale étendue	• Implémente un saut à jetons	<#root>

	avec des fonctionnalités de rafale étendue. • Désactivé en définissant BC = Be. • Lorsque BC est égal à Be, le régulateur du trafic ne peut pas emprunter de jetons et il supprime simplement le paquet si le nombre de jetons disponibles est insuffisant.	`2 * normal burst`

Toutes les plates-formes n'utilisent pas ou ne prennent pas en charge la même plage de valeurs pour un régulateur. Consultez le document suivant pour connaître les valeurs prises en charge pour votre plate-forme spécifique :

- Vue d'ensemble de la réglementation et du formatage

Q. Comment la réglementation CAR (Committed Access Rate) ou basée sur les classes détermine-t-elle si un paquet est conforme ou dépasse le CIR (Committed Information Rate) ? Le routeur supprime des paquets et signale un débit dépassé même si le débit conforme est inférieur au CIR configuré.

R. Un régulateur de trafic utilise les valeurs de rafale normale et de rafale étendue pour s’assurer que le CIR configuré est atteint. Il est important de définir des valeurs de rafale suffisamment élevées de façon à garantir un débit correct. Si les valeurs de rafale ne sont pas suffisamment élevées, le débit obtenu peut être largement inférieur au débit configuré. Les rafales provisoires peut avoir une incidence fortement défavorable sur le débit du trafic TCP. Avec le CAR, émettez la commande show interface rate-limit pour contrôler la rafale actuelle et déterminer si la valeur affichée est constamment proche des valeurs BC et Be.

<#root>

```
rate-limit 256000 7500 7500 conform-action continue exceed-action drop
rate-limit 512000 7500 7500 conform-action continue exceed-action drop
```

```
router#
```

show interfaces virtual-access 26 rate-limit

```
    Virtual-Access26 Cable Customers
      Input
        matches: all traffic
          params:  256000 BPS, 7500 limit, 7500 extended limit
          conformed 2248 packets, 257557 bytes; action: continue
          exceeded 35 packets, 22392 bytes; action: drop
          last packet: 156ms ago, current burst: 0 bytes
          last cleared 00:02:49 ago, conformed 12000 BPS, exceeded 1000 BPS
      Output
        matches: all traffic
```

params: 512000 BPS

```
, 7500 limit, 7500 extended limit
          conformed 3338 packets, 4115194 bytes; action: continue
          exceeded 565 packets, 797648 bytes; action: drop
          last packet: 188ms ago,
```

current burst: 7392 bytes

```
          last cleared 00:02:49 ago,
```

conformed 194000 BPS, exceeded 37000 BPS

Pour plus d'informations, référez-vous aux documents suivants :

- Vue d'ensemble de la réglementation et du formatage
- Réglementation QoS sur la gamme Catalyst 6000
- Forum aux questions sur la qualité de service de la gamme Catalyst 4000
- QoS (Qualité de service) des commutateurs Catalyst G-L3 et des modules WS-X4232-L3 de couche 3 - Forum Aux Questions

Q. Les limites de rafale et de file d'attente sont-elles indépendantes l'une de l'autre ?

R. Oui, la rafale du régulateur et la limite de file d'attente sont séparées et indépendantes l'une de l'autre. Vous pouvez considérer le régulateur comme une porte qui autorise un certain nombre de paquets (ou octets) et la file d'attente comme un saut de taille queue limit qui contient les paquets admis avant la transmission sur le réseau. Idéalement, vous voulez que votre saut soit suffisamment grand pour contenir une rafale des octets/paquets admis par la porte (régulateur).

Qualité de service (QoS) des relais de trame

Q. Quelles valeurs dois-je sélectionner pour le débit garanti (CIR), la rafale garantie

(BC), la rafale excédentaire (Be) et le débit minimal garanti (MinCIR) ?

R. La mise en forme du trafic Frame Relay, que vous activez en exécutant la commande frame-relay traffic-shaping, prend en charge plusieurs paramètres configurables. Ces paramètres incluent `frame-relay cir`, `frame-relay mincir` et `frame-relay BC`. Consultez les documents suivants pour plus d'informations sur la sélection de ces valeurs et une présentation des commandes show associées :

- Configuration du formatage de trafic de relais de trame sur les routeurs 7200 et plates-formes inférieures
- Commandes show pour le formatage du trafic Frame Relay
- VoIP sur relais de trame avec qualité de service (fragmentation, formatage du trafic, IP RTP Priority)

Q. La mise en file d'attente prioritaire sur l'interface principale Frame Relay fonctionne-t-elle dans Cisco IOS 12.1 ?

R. Les interfaces Frame Relay prennent en charge les mécanismes de mise en file d'attente d'interface et les mécanismes de mise en file d'attente par circuit virtuel (VC). À partir de Cisco IOS 12.0(4)T, la file d'attente d'interface ne prend en charge la mise en file d'attente First In First Out (FIFO) ou la mise en file d'attente par priorité (PQ) par interface que lorsque vous configurez le formatage du trafic Frame Relay (FRTS). Par conséquent, la configuration suivante ne fonctionnera plus si vous effectuez une mise à niveau vers Cisco IOS 12.1.

```
interface Serial0/0
  frame-relay traffic-shaping
  bandwidth 256
  no ip address
  encapsulation frame-relay IETF
  priority-group 1

 !
 interface Serial0/0.1 point-to-point
  bandwidth 128
  ip address 136.238.91.214 255.255.255.252
  no ip mroute-cache
  traffic-shape rate 128000 7936 7936 1000
  traffic-shape adaptive 32000
  frame-relay interface-dlci 200 IETF
```

Si FRTS n'est pas activé, vous pouvez appliquer une autre méthode de mise en file d'attente, telle que la mise en file d'attente pondérée basée sur les classes (CBWFQ), à l'interface principale, laquelle agit comme un canal de bande passante unique. En outre, depuis Cisco IOS 12.1.1(T), vous pouvez activer la mise en file d'attente d'interface prioritaire (PIPQ) de circuits virtuels permanents (PVC) Frame Relay sur une interface principale Frame Relay. Vous pouvez définir des PVC de priorité élevée, moyenne, normale ou basse et émettre la commande frame-relay

interface-queue priority sur l'interface principale, comme dans l'exemple suivant :

<#root>

```
interface Serial3/0
 description framerelay main interface
 no ip address
 encapsulation frame-relay
 no ip mroute-cache
 frame-relay traffic-shaping

frame-relay interface-queue priority

interface Serial3/0.103 point-to-point
 description frame-relay subinterface
 ip address 1.1.1.1 255.255.255.252
 frame-relay interface-dlci 103
  class frameclass

map-class frame-relay frameclass
 frame-relay adaptive-shaping becn
 frame-relay cir 60800
 frame-relay BC 7600
 frame-relay be 22800
 frame-relay mincir 8000
 service-policy output queueingpolicy

frame-relay interface-queue priority low
```

Q. Frame Relay Traffic Shaping (FRTS) fonctionne-t-il avec Distributed Cisco Express Forwarding (dCEF) et Distributed Class Based Weighted Fair Queueing (dCBWFQ) ?

R. Depuis la version 12.1(5)T de la plate-forme logicielle Cisco IOS, seule la version distribuée des fonctions QoS est prise en charge sur les VIP de la gamme Cisco 7500. Pour permettre le formatage du trafic sur des interfaces de relais de trame, utilisez le Distributed Traffic Shaping (DTS). Pour plus d'informations, référez-vous aux documents suivants :

- FRF.11 et FRF.12 Versatile Interface Processor distribués pour Cisco IOS Version 12.1 T
- Mise en forme du trafic de relais de trame avec QoS distribué sur Cisco 7500

Qualité de service (QoS) sur mode de transfert asynchrone (ATM)

Q. Où dois-je appliquer une politique de service avec CBWFQ (Class Based Weighted Fair Queueing) et LLQ (Low Latency Queueing) sur une interface ATM

(Asynchronous Transfer Mode) ?

R. Depuis Cisco IOS 12.2, les interfaces ATM prennent en charge des politiques de service à trois niveaux ou interfaces logiques : interface principale, sous-interface et circuit virtuel permanent (PVC). L'emplacement auquel vous appliquez la stratégie est conditionnée par la fonction de qualité de service (QoS) que vous activez. Les stratégies de mise en file d'attente doivent être appliquées par circuit virtuel (VC) puisque l'interface ATM contrôle le niveau de congestion par circuit virtuel et gère les files d'attente des paquets excédentaires par circuit virtuel. Pour plus d'informations, référez-vous aux documents suivants :

- Application d'une stratégie de service QoS sur une interface ATM
- Présentation de la mise en file d'attente de transmission par circuit virtuel sur les interfaces ATM PA-A3 et NM-1A

Q. Quels octets sont comptés par les files d’attente de classe de service (CO) IP à ATM (Asynchronous Transfer Mode) ?

R. Les commandes bandwidth et priority configurées dans une politique de service pour activer la mise en file d'attente pondérée basée sur les classes (CBWFQ) et la mise en file d'attente à faible latence (LLQ), respectivement, utilisent une valeur Kbits/s qui compte les mêmes octets de surcharge que ceux comptés par la sortie de commande show interface. En particulier, le système de mise en file d'attente de couche 3 prend en compte le contrôle de la liaison logique / protocole d'accès au sous-réseau (LLC/SNAP). Il ne prend pas en compte ce qui suit :

- Trailer de la couche d'adaptation ATM 5 (AAL5)
- Remplissage pour faire de la dernière cellule un multiple pair de 48 octets
- En-tête de cellule de cinq octets
- Quels sont les octets pris en compte par la mise en file d'attente CoS d'IP à ATM

Q. Combien de circuits virtuels (VCS) peuvent prendre en charge une politique de service simultanément ?

R. Le document suivant fournit des directives utiles sur le nombre de VCS ATM (Asynchronous Transfer Mode) pouvant prendre en charge. Environ 200 à 300 circuits virtuels permanents vbr-nrt (PVC) VBR-nrt ont été déployés en toute sécurité :

- Guide de conception de la classe de service IP à ATM

Prenez en compte également ce qui suit :

- Utilisez un processeur de forte capacité. Par exemple, un VIP4-80 fournit de manière significative des performances plus élevées qu'un VIP2-50.
- Quantité de mémoire de paquets disponible. Sur le NPE-400, jusqu'à 32 Mo (dans un

système de 256 Mo) sont réservés pour la mémoire tampon des paquets. Pour un NPE-200, jusqu'à 16 Mo sont réservés pour des mémoires tampon de paquets sur un système de 128 Mo.

- Des configurations avec la Weighted Random Early Detection (WRED) par circuit virtuel fonctionnant simultanément sur un maximum de 200 circuits virtuels ATM ont été intensivement testées. La quantité de mémoire de paquets sur le VIP2-50 pouvant être utilisée pour les files d'attente par circuit virtuel est limitée. Par exemple, un VIP2-50 avec 8 Mo de SRAM fournit 1 085 mémoires tampon de paquets disponibles pour la mise en file d'attente par circuit virtuel de classe de service IP à ATM sur lesquelles la WRED fonctionne. Si 100 PVC ATM ont été configurés et si tous les circuits virtuels ont simultanément fait l'objet d'une congestion excessive (comme cela pourrait être simulé dans des environnements de test où une source contrôlée par un flux autre que TCP serait utilisée), chaque PVC aurait en moyenne une mise en mémoire tampon d'environ 10 paquets, ce qui peut être insuffisant pour que la WRED fonctionne correctement. Les périphériques VIP2-50 avec une SRAM importante sont donc fortement recommandés dans les conceptions comportant un nombre élevé de circuits virtuels ATM exécutant des WRED par circuit virtuel et pouvant faire simultanément l'objet de congestion.

- Plus le nombre de PVC configurés actifs est élevé, plus le nombre de Sustained Cell Rate (SCR) devra être faible, et par conséquent, plus la file d'attente requise par la WRED pour fonctionner sur le PVC devra être courte. Ainsi, comme cela est le cas lors de l'utilisation des profils WRED par défaut de la fonction de phase 1 de classe de service (COs) IP à ATM, la configuration de seuils inférieurs de suppression de WRED lorsque la WRED par circuit virtuel est activée sur un très grand nombre de PVC lents congestionnés réduirait le risque de pénurie de mémoire tampon sur le VIP. La pénurie de mémoire tampon sur le VIP n'entraîne aucun dysfonctionnement. Dans le cas de pénurie de mémoire tampon sur le VIP, la fonction de phase 1 de COs d'IP à ATM passe simplement au « tail drop » First In First Out (FIFO) durant la pénurie de mémoire tampon (c'est-à-dire la même stratégie de suppression qui serait utilisée si la fonction de COs d'IP à ATM n'était pas activée sur ce PVC).

- Nombre maximal de circuits virtuels simultanés qui peut être raisonnablement pris en charge.

Q. Quel matériel ATM (Asynchronous Transfer Mode) prend en charge les fonctions de classe de service (CO) IP à ATM, notamment CBWFQ (Class-Based Weighted Fair Queueing) et LLQ (Low Latency Queueing) ?

R. Les centraux téléphoniques IP vers ATM font référence à un ensemble de fonctionnalités activées par circuit virtuel (VC, Virtual Circuit). La COs IP à ATM n'est donc pas prise en charge sur le processeur d'interface ATM (AIP), ou sur les processeurs réseau ATM 4500 ou PA-A1. Ce matériel ATM ne prend pas en charge la mise en file d'attente par circuit virtuel, telle que le PA-A3 et la plupart des modules réseau (autres que l'ATM-25) la définissent. Pour plus d'informations, reportez-vous au document suivant :

- Présentation de la prise en charge de matériel ATM pour la classe de service IP à ATM

- Mise en file d'attente pondérée basée sur les classes par circuit virtuel sur les plates-formes basées sur un processeur de commutation routage (RSP)
- Mise en file d'attente pondérée basée sur les classes par circuit virtuel (Per-VC CBWFQ) sur les routeurs Cisco 7200, 3600 et 2600
- Mise en file d'attente par circuit virtuel sur l'adaptateur de port ATM PA-A3-8T1/E1 IMA
- Configuration de la mise en file d'attente par circuit virtuel ATM sur le MC3810

Voix et qualité de service (QoS)

Q. Comment fonctionne la fragmentation et l’entrelacement de liens (LFI) ?

R. Le trafic interactif, tel que Telnet et Voice over IP, est susceptible d’augmenter la latence lorsque le réseau traite des paquets volumineux, tels que les transferts FTP (File Transfer Protocol) sur un réseau étendu. Le délai de paquets pour le trafic interactif est significatif lorsque les paquets FTP sont placés en file d'attente sur des liaisons WAN plus lentes. Une méthode a été conçue pour fragmenter les paquets les plus grands, et placer en file d'attente les paquets les plus petits (voix) entre les fragments des paquets les plus grands (FTP). Les routeurs Cisco IOS prennent en charge plusieurs mécanismes de fragmentation de la couche 2. Pour plus d'informations, référez-vous aux documents suivants :

- Vue d'ensemble des mécanismes d'efficacité de liaison
- VoIP sur relais de trame avec qualité de service (fragmentation, formatage du trafic, IP RTP Priority)
- VoIP sur liaisons PPP avec qualité de service (LLQ / IP RTP Priority, LFI, cRTP)

Q. Quels outils puis-je utiliser pour surveiller les performances de la voix sur IP ?

R. Cisco propose actuellement plusieurs options de surveillance de la qualité de service (QoS) dans les réseaux utilisant les solutions de voix sur IP de Cisco. Ces solutions ne mesurent pas la qualité vocale à l'aide de la méthode Perceptual Speech Quality Measurement (PSQM) ou de certains des nouveaux algorithmes proposés pour mesurer la qualité vocale. Les outils Agilent (HP) et NetIQ sont disponibles à cet effet. Cisco offre cependant des outils qui donnent une idée de la qualité vocale que vous obtenez en mesurant le délai, la gigue et la perte de paquets. Pour plus d'informations, consultez Utilisation du Service Assurance Agent et de l'Internetwork Performance Monitor de Cisco pour gérer la qualité de service sur des réseaux Voix sur IP.

Q. %SW_MGR-3-CM_ERROR_FEATURE_CLASS : Connection Manager Feature Error: Class SSS: (QoS) - install error, ignore.

R. L'erreur d'installation de fonctionnalité observée est un comportement attendu lorsqu'une configuration non valide est appliquée à un modèle. Elle indique que la stratégie de service n'a pas été appliquée en raison d'un conflit. Vous ne devez généralement pas configurer le formatage

sur la valeur par défaut des classes de la stratégie enfant dans les mappages de stratégies hiérarchiques ; configurez-le sur la stratégie parente de l'interface. L'impression et le traçage de ce message en sont la conséquence.

Avec des stratégies basées sur les sessions, le formatage des valeurs par défaut des classes doit être uniquement effectué au niveau PVC de la sous-interface. La formatage de l'interface physique n'est pas pris en charge. Si la configuration est effectuée sur l'interface physique, l'occurrence de ce message d'erreur est un comportement attendu.

Dans le cas de LNS, une autre raison pourrait être que la stratégie de service peut être fournie par l'intermédiaire du serveur RADIUS lorsque les sessions sont démarrées. Émettez la commande show tech pour afficher la configuration du serveur RADIUS et toutes les stratégies de service illégales qui sont installées par l'intermédiaire du serveur RADIUS lorsque la session s'ouvre ou devient instable.

Informations connexes

- Notions de base de l'optimisation des performances
- Prise en charge de la qualité de service (QoS)
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.